From: Jon Abbey
To: Microsoft ATR
Date: 1/23/02 12:13pm
Subject: Comments on Microsoft settlement

To whom it may concern,

I am a computer professional who has worked in the industry for a
decade, and who has closely observed Microsoft's practices in the
industry since the early 1980's. I am writing to request that the
settlement proposed by the DOJ, Microsoft, and the consenting states be
rejected as inadequate to the damage done by Microsoft.

Microsoft has been so successful in driving out all competition from the
market through the power of their control over the PC platform that in
many cases the only viable remaining sources of competing innovation has
come from so-called free software. Free software, or Open Source,
refers to software products like Linux or Apache or Mozilla, or FreeBSD,
in which a global community of developers contribute their time and
energy to sustaining software projects as a resource to the public.

It is unacceptable, therefore, that the proposed settlement stipulates
that Microsoft be obliged to share details of their secret data formats
and networking protocols only to those commercial interests that
Microsoft deems worthy to receive that information. Such language in
the proposed settlement is designed entirely to shield Microsoft from
the volunteer workers who can not be bought or put out of business by
Microsoft's huge cash reserves and industry leverage.

It is likewise unacceptable that Microsoft be given the ability to
withhold any protocol information that might be related to their
security mechanisms. It is, of course, true that information that could
lead to the compromise of access controls on computer systems running
Microsoft software would be damaging to Microsoft and the public. It is
not true, however, that any revelation of protocols will have this
result. Every web browser that supports encrypted communication with a
web server does so through an open, industry standard protocol known as
TLS. TLS is an extraordinarily well documented standard, and there are
scores of individual programs on many different computer and operating
systems that work with TLS. This does not in any way negatively impact
the security of the TLS protocol. A security protocol is not secure
because it is secret, it is secure because the mathematics of the system
make it vastly impractical that anyone could muster enough computer
power to decrypt a given communications stream.

Microsoft should be required to document their networking protocols in
full, so that others, both commercial interests and volunteer
developers, can create products to fully interoperate in a compatible
fashion with Microsoft systems.

At the very least, independent technical experts not under Microsoft's pay or control should be consulted so that these two loopholes in the proposed settlement may be properly closed.

Thank you,

  Jonathan Abbey

Jonathan Abbey   - jonabbey@burrow.org -   Austin, TX